

Listing of the Claims:

The following is a complete listing of all the claims in the application, with an indication of the status of each:

- 1 1. (Currently Amended) An electronic circuit for cryptographic processing,
2 comprising:
3 a first combinatorial logical circuit, having an input, arranged to
4 perform a first set of logical operations on an input data at the input and to
5 produce a corresponding first output data, the first output data having a first
6 ~~given~~ functional relation to the input data for said input data within a given
7 range; and
8 a second combinatorial logical circuit, having an input, arranged to
9 perform a second set of logical operations on an input data at said input and to
10 produce a corresponding second output data, the second output data having a
11 second functional relation to said the input data, said second functional
12 relation identical to said first ~~the given~~ functional relation for said input data
13 within said given range,
14 wherein the first set of logical operations is different from the second set
15 of logical operations, and
16 a selector for receiving a given input data and dynamically selecting
17 from among the first combinatorial logical circuit for performing the first set of
18 logical operations on the given input data and the second combinatorial logical

19 circuit for performing the second set logical operations on the given input data
20 and producing output data, and

21 wherein the selecting includes inputting the given input data to the
22 input of the selected one of the first and second combinatorial logical
23 circuits and outputting a selected first cryptographic processing output, the
24 selected first cryptographic processing output being the output of the
25 selected one of the first and second combinatorial logical circuits.

1 2. (Currently Amended) The electronic circuit according to claim 1, further
2 comprising:

3 a third combinatorial logical circuit, having an input, arranged to
4 perform a third set of logical operations on an input data at said input and to
5 produce a corresponding output data, the output data having a third given
6 functional relation to said input data for input data within a given range, and

7 a fourth combinatorial logical circuit, having an input, arranged to
8 perform a fourth set of logical operations on an input data at said input and to
9 produce a corresponding output data, ~~the~~ said output data having a fourth
10 functional relation to said input data identical to said third given functional
11 relation for input data within said given range,

12 wherein the third set of logical operations is different from the fourth
13 set of logical operations, and

14 a selector for receiving said selected first cryptographic processing
15 output data and dynamically selecting from among the third combinatorial
16 logical circuit and the fourth combinatorial logical circuit for performing logical
17 operations on the selected first cryptographic processing output data and
18 producing a second output cryptographic processing data, and
19 wherein said selecting includes inputting the selected first
20 cryptographic processing output data to the input of the selected one of the
21 third and fourth combinatorial logical circuits.

1 3. (Currently Amended) The electronic circuit of claim 1, wherein the selector
2 comprises:

3 a selection circuit for generating a selecting signal to select one
4 combinatorial logical circuit from among ~~of~~ the first and second ~~set of~~
5 combinatorial logical circuits

6 a splitter circuit for inputting the given input data to one of the first and
7 second combinatorial logical circuits, depending on the signal,

8 a merger circuit for outputting data from one of the first and second
9 combinatorial logical circuits, depending on the selecting signal.

1 4. (Currently Amended) The electronic circuit of claim 3, further
2 comprising a timing circuit to determine the points in time at which the

3 selection circuit generates the selecting signal to select one of the first and
4 second combinatorial logical combinatorial logical circuits.

1 5. (Currently Amended) An electronic circuit for cryptographic processing,
2 comprising:

3 a combinatorial logical circuit to perform logical operations on input
4 data and to produce an output data,

5 a storage circuit for storing the output data produced by the
6 combinatorial logical circuit,

7 wherein the storage circuit comprises

8 a first encoding means for encoding the output data into a first encoded
9 output data,

10 a storage element for retrievably storing the first encoded output data,

11 a corresponding first decoding means, arranged for decoding the first
12 encoded output data into said output data after retrieving the first encoded
13 output data from the storage element, and

14 wherein the electronic circuit is arranged to dynamically control the
15 activation of the first an encoding means and the corresponding first
16 decoding means.

1 6. (Currently Amended) The electronic circuit of claim 5, wherein the storage
2 circuit further comprises:

3 a second encoding means for encoding the output data into a second
4 encoded output data for storing in the storage element,
5 a corresponding second decoding means, arranged for decoding the
6 second encoded output data into said output data after retrieving the second
7 encoded output data from the storage element,
8 wherein the encoding of the first output data is different from the
9 encoding of the second output data, and
10 wherein the electronic circuit is further arranged to generate a
11 selecting signal to dynamically select from among the first encoding means
12 and its corresponding first decoding means and the second encoding means
13 and its corresponding second decoding means, for encoding and decoding of
14 the output data.

1 7. (Previously Presented) The electronic circuit of claim 6, further
2 comprising a timing circuit to determine the points in time at which the
3 electronic circuit selects one from among the first and second encoding
4 means and corresponding first and second decoding means.

1 8. (Currently Amended) The electronic circuit of claim 6 [[5]], wherein the
2 combinatorial logical circuit comprises:

3 a first combinatorial logical circuit, having an input, arranged to
4 perform a first set of logical operations on input data at the input and to

5 produce a corresponding cryptographic output data, the cryptographic output
6 data having a given first functional relation to the input data for said input
7 data within a given range, and

8 a second combinatorial logical circuit, having an input, arranged to
9 perform a second set of logical operations on input data at said input and to
10 produce a second cryptographic output data, the second cryptographic output
11 data having a second functional relation to the input data, said second
12 functional relation identical to said first ~~the given~~ functional relation for said
13 input data within said given range,

14 wherein the selecting includes inputting the ~~given~~ input data to the
15 input of the selected one of the first and second combinatorial logical circuits
16 and outputting a selected output, the selected output being the output of the
17 selected one of the first and second combinatorial logical circuits.

9. (Canceled)

1 10. (Previously Presented) A method of processing cryptographic data,
2 comprising:

3 using a set of logical operations for processing input data and producing
4 output data,

5 storing the output data in a storage element, wherein the storing
6 comprises:

7 encoding the output data into an encoded output data,
8 storing the encoded output data in the storage element,
9 retrieving the encoded output data from the storage element,
10 decoding the encoded output data retrieved from the storage
11 element, and
12 dynamically controlling the encoding of the output data into an
13 encoded output data and the corresponding decoding of the encoded
14 output data retrieved from the storage element.

11. (Canceled)

1 12. (Currently Amended) The electronic circuit of claim 3 [[1]], wherein the
2 selector includes:

3 a first mask circuit for selectively masking and not masking, based on
4 the selecting signal, the given input data for input to the first combinatorial
5 logical circuit, and

6 a second mask circuit for selectively masking and not masking, based
7 on the selecting signal, the given input data for input to the second
8 combinatorial logical circuit.

1 13. (Currently Amended) The electronic circuit of claim 8, wherein the selector
2 includes:

3 a first mask circuit to selectively mask and not mask, based on the
4 selecting signal, the given input data and to input the selected masked and not
5 masked given input data to the first combinatorial logical circuit, and
6 a second mask circuit to selectively mask and not mask, based on the
7 selecting signal, to input the selected masked and not masked given input data
8 to the second combinatorial logical circuit.

1 14. (Previously Presented) The electronic circuit of claim 13,
2 wherein the first mask circuit includes an AND mask configured to
3 mask and to not mask the given input data by inputting to the first
4 combinatorial logical circuit a selection between all zeros and the given input
5 data, respectively and

6 wherein the second mask circuit includes an AND mask configured
7 to mask and to not mask the given input data by inputting to the second
8 combinatorial logical circuit a selection between all zeros and the given
9 input data, respectively.

1 15. (Previously Presented) The electronic circuit of claim 1, wherein the
2 selector includes an OR merger circuit to receive the output of the first
3 combinatorial logical circuit and to receive the output of the second
4 combinatorial logic circuit, and to output, as the selected output, a logical

5 OR of the output of the first combinatorial logical circuit and the output of
6 the second combinatorial logic circuit.

1 16. (Currently Amended) A method of processing cryptographic data,
2 comprising:

3 generating a mode signal having one of a given plurality of states;

4 receiving a given input data and generating a cryptographic processed
5 data output, said generating including:

6 generating a first input data, wherein the first input data is a
7 selected one of a mask of the given input data and a not mask of the
8 given input data, the selection based on the state of the mode signal;

9 generating a second input data, wherein the second input data is
10 the other of the mask of the given input data and the not mask of the
11 given input data, performing a first set of logical operations on the first
12 input data to generate a first output data, the first set of logical
13 operations embodying a given input-output function,

14 performing a second set of logical operations on the second input
15 data to generate a second output data, the second set of logical
16 operations being different than the first set of logical operations and the
17 second set of logical operations embodying the same given input-output
18 function, and

19 merging the first output data and the second output data to
20 generate the cryptographic data output;
21 repeating said generating a mode signal to have a different one of the
22 given plurality of states; and
23 repeating said receiving a given input data and generating a
24 cryptographic processed data output.

1 17. (New) The electronic circuit of claim 1,
2 wherein the first combinatorial logical circuit comprises a first
3 configuration of logical gates receiving a given power supply current, having
4 an input, arranged to receive an input data A at said input and generate a
5 cryptographic output data $= f(A)$, f being a given function, by performing $f(A)$
6 as a first set of logical operations on said first configuration of logical gates,
7 wherein said first configuration and said first set of logical operations
8 are configured to generate a first power consumption profile when performing
9 $f(A)$, and
10 wherein the first combinatorial logical circuit comprises a second
11 configuration of logical gates receiving a given power supply current, having
12 an input, arranged to receive an input data A at said input and generate a
13 cryptographic output data $= g(A)$, g being a given function, wherein $g(A) = f(A)$
14 for all A in a given range of A , by performing $g(A)$ as a second set of logical
15 operations on said second configuration of logical gates, and

16 wherein said second configuration and said second set of logical
17 operations are configured to generate a second power consumption profile
18 when performing $g(A)$ different from the first power consumption profile in
19 performing $f(A)$.

1 18. (New) The electronic circuit of claim 17,

2 wherein the selector is configured for receiving a given input data A
3 and dynamically selecting from among the first combinatorial logical circuit
4 for performing said $f(A)$ = the cryptographic output data and the second
5 combinatorial logical circuit for performing said $g(A)$ = the cryptographic
6 output data and producing a selected cryptographic output data as a
7 selected one of either of $f(A)$ and $g(A)$, based said dynamic selecting.

1 19. (New) The electronic circuit of claim 1,

2 wherein the first combinatorial logical circuit comprises a first
3 configuration of AND, OR and NOT logical gates receiving a given power
4 supply current, having an input, arranged to receive an input data A at said
5 input and generate a cryptographic output data = $f(A)$, f being a given function,
6 by performing $f(A)$ as a first set of logical AND, OR and NOT operations on
7 said first configuration of AND, OR and NOT logical gates, and

8 wherein the second combinatorial logical circuit comprises a second
9 configuration of AND, OR and NOT logical gates receiving a given power

10 supply current, having an input, arranged to receive an input data A at said
11 input and generate a cryptographic output data $= g(A)$, g being a given
12 function, wherein $g(A) = f(A)$ for all A in a given range of A , by performing
13 $g(A)$ as a second set of logical AND, OR and NOT operations on said second
14 configuration of AND, OR and NOT logical gates, and
15 wherein said second configuration and said second set of logical AND,
16 OR and NOT operations are different from said first configuration and said
17 first set of logical AND, OR and NOT operations.

1 20. (New) The electronic circuit of claim 19,
2 wherein the selector is configured to receive the given input data A and
3 dynamically select from among the first combinatorial logical circuit for
4 performing said $f(A)$ = the cryptographic output data and the second
5 combinatorial logical circuit for performing said $g(A)$ = the cryptographic
6 output data and to produce a selected cryptographic output data as a selected
7 one of $f(A)$ and $g(A)$, based on said dynamic selecting.

1 21. (New) The electronic circuit of claim 20,
2 wherein the first combinatorial logical circuit comprises a first
3 configuration of AND, OR and NOT logical gates receiving a given power
4 supply current, having an input, arranged to receive an input data A at said
5 input and generate a cryptographic output data $= f(A)$, f being a given function,

6 by performing $f(A)$ as a first set of logical AND, OR and NOT operations on
7 said first configuration of AND, OR and NOT logical gates, wherein said first
8 configuration and said first set of logical AND, OR and NOT operations are
9 configured to generate a first power consumption profile when performing $f(A)$,

10 and

11 wherein the second combinatorial logical circuit comprises a second
12 combinatorial logical circuit comprising a second configuration of AND, OR
13 and NOT logical gates receiving a given power supply current, having an
14 input, arranged to receive an input data A at said input and generate a
15 cryptographic output data $= g(A)$, g being a given function, wherein $g(A) = f(A)$
16 for all A in a given range of A , by performing $g(A)$ as a second set of logical
17 AND, OR and NOT operations on said second configuration of AND, OR and
18 NOT logical gates, and

19 wherein said second configuration and said second set of logical AND,
20 OR and NOT operations are different from said first configuration and said
21 first set of logical AND, OR and NOT operations and wherein said second
22 configuration and said second set of logical AND, OR and NOT operations are
23 configured to generate a second power consumption profile when performing
24 $g(A)$ and, wherein, for a given A , the first power consumption profile in
25 performing $f(A)$ is different from the second power consumption profile in
26 performing $g(A)$.

1 22. (New) The electronic circuit of claim 2,

2 wherein the first combinatorial logical circuit comprises a first
3 configuration of AND, OR and NOT logical gates receiving a given power
4 supply current, having an input, arranged to receive an input data A at said
5 input and generate a cryptographic output data $= f(A)$, f being a given function,
6 by performing $f(A)$ as a first set of logical AND, OR and NOT operations on
7 said first configuration of AND, OR and NOT logical gates, wherein said first
8 configuration and said first set of logical AND, OR and NOT operations are
9 configured to generate a first power consumption profile when performing $f(A)$,

10 wherein the second combinatorial logical circuit comprises a second
11 combinatorial logical circuit comprising a second configuration of AND, OR
12 and NOT logical gates receiving a given power supply current, having an
13 input, arranged to receive an input data A at said input and generate a
14 cryptographic output data $= g(A)$, g being a given function, wherein $g(A) = f(A)$
15 for all A in a given range of A , by performing $g(A)$ as a second set of logical
16 AND, OR and NOT operations on said second configuration of AND, OR and
17 NOT logical gates, and

18 wherein said second configuration and said second set of logical AND,
19 OR and NOT operations are different from said first configuration and said
20 first set of logical AND, OR and NOT operations,

21 wherein said second configuration and said second set of logical AND,
22 OR and NOT operations are configured to generate a second power

23 consumption profile when performing $g(A)$ and, wherein, for a given A , the
24 first power consumption profile in performing $f(A)$ is different from the second
25 power consumption profile in performing $g(A)$,

26 wherein the third combinatorial logical circuit comprises a third
27 configuration of AND, OR and NOT logical gates receiving a given power
28 supply current, having an input, arranged to receive an input data B at said
29 input and generate a cryptographic output data $= f1(B)$, $f1$ being a given
30 function, by performing $f1(B)$ as a third set of logical AND, OR and NOT
31 operations on said third configuration of AND, OR and NOT logical gates,

32 wherein said third configuration and said third set of logical AND, OR
33 and NOT operations are configured to generate a third power consumption
34 profile when performing $f1(A)$, and

35 a fourth combinatorial logical circuit comprising a fourth configuration
36 of AND, OR and NOT logical gates receiving a given power supply current,
37 having an input, arranged to receive an input data B at said input and
38 generate a cryptographic output data ,

39 wherein said cryptographic output data $= g1(B)$, $g1$ being a given
40 function, wherein $g1(B) = f1(B)$ for all B in a given range of B , by performing
41 $g1(B)$ as a fourth set of logical AND, OR and NOT operations on said fourth
42 configuration of AND, OR and NOT logical gates,

43 wherein said fourth configuration and said fourth set of logical AND, OR
44 and NOT operations are different from said third configuration and said third
45 set of logical AND, OR and NOT operations,

46 wherein said fourth configuration and said fourth set of logical AND, OR
47 and NOT operations are configured to generate a fourth power consumption
48 profile when performing $g1(B)$ and,

49 wherein, for a given B, the third power consumption profile in
50 performing $f1(B)$ is different from the fourth power consumption profile in
51 performing $g1(B)$.